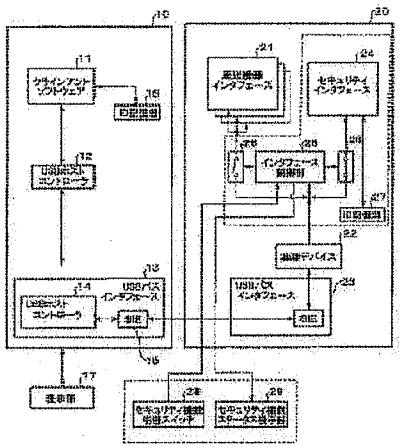
COMPUTER SYSTEM EQUIPPED WITH USB DEVICE WITH SECURITY FUNCTION

Publication number: JP2003186819 (A)
Publication date: 2003-07-04
Inventor(s): HIRANO ATSUSHI +
Applicant(s): RICOH KK +
Classification:
- international: ***G06F1/00; G06F13/14; G06F15/00; G06F21/20;*** **G06F1/00; G06F13/14; G06F15/00; G06F21/20;** (IPC1-7): G06F1/00; G06F13/14; G06F15/00
- European:
Application number: JP20010382487 20011217
Priority number(s): JP20010382487 20011217

Abstract of **JP 2003186819 (A)**

PROBLEM TO BE SOLVED: To provide a computer system equipped with a USB (universal serial bus) device with a security function, comprised of the USB device having a security function and a computer capable of using the USB. ; SOLUTION: A personal computer (PC) 10 has a client software 11 provided with an ID storage part 16, a USB host controller 14 and the like. The USB device 20 has a peripheral equipment interface 21 to achieve an intrinsic function as peripheral equipment, a security interface 24 equipped with an ID storage part 27, an interface control part 25 to control the peripheral equipment interface 21 and the security interface 24, a USB bus interface 23, and the like. By the time when the use of the USB device 20 get authenticated by the PC 10 based on the comparison of IDs of both sides, the state of the security interface 24 becomes to be able to return a descriptor and the state of the peripheral equipment interface 21 becomes not to be able to return a descriptor. ; COPYRIGHT: (C)2003,JPO



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－186819
（P2003－186819A）
(43)公開日　平成15年７月４日(2003.7.4)

(51)Int.Cl.[7]		識別記号	FI		テーマコード*(参考)
Ｇ０６Ｆ	13/14	３３０	Ｃ０６Ｆ 13/14	３３０Ｃ	５Ｂ０１４
	1/00	３７０	1/00	３７０Ｅ	５Ｂ０８５
	15/00	３３０	15/00	３３０Ｃ	

審査請求　未請求　請求項の数５　ＯＬ　（全 ９ 頁）

(21)出願番号　特願2001－382487(P2001－382487)

(22)出願日　平成13年12月17日(2001.12.17)

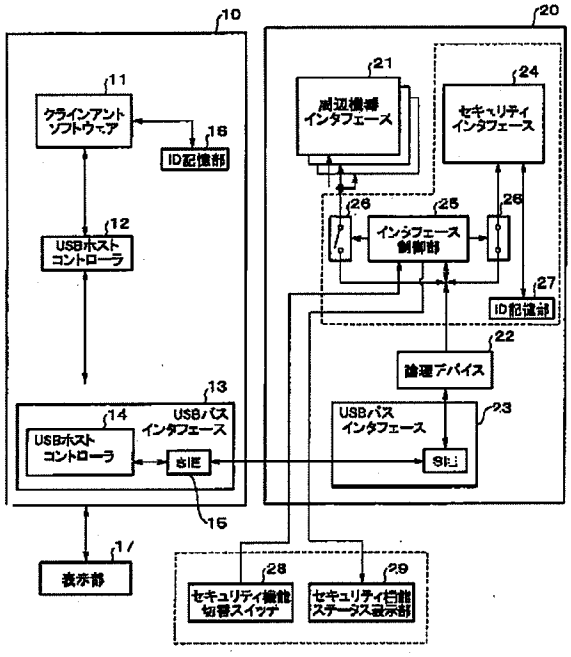
(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号

(72)発明者　平野　敦
東京都大田区中馬込１丁目３番６号　株式会社リコー内

Ｆターム(参考)　5B014 EB03 FA05 FB04 GD05 GD22
GD34 GE05 HC04 HC08 HC13
5B085 AE04

(54)【発明の名称】　セキュリティ機能付きＵＳＢ機器を備えたコンピュータシステム

(57)【要約】
【課題】　セキュリティ機能を有するＵＳＢ機器と該ＵＳＢ機器を使用可能なコンピュータからなるセキュリティ機能付きＵＳＢ機器を備えたコンピュータシステムを提供する。
【解決手段】　パーソナルコンピュータ（ＰＣ）１０は、ＩＤ記憶部１６を備えたクライアントソフトウェア１１，ＵＳＢホストコントローラ１４等を有する。ＵＳＢ機器２０は、周辺機器としての本来の機能を実現する周辺機器インタフェース２１，ＩＤ記憶部２７を備えたセキュリティインタフェース２４，周辺機器インタフェース２１とセキュリティインタフェース２４を制御するインタフェース制御部２５，ＵＳＢバスインタフェース２３等を有する。双方のＩＤの比較により、ＵＳＢ機器２０の使用がＰＣ１０により認証されるまで、セキュリティインタフェース２４がディスクリプタを返せる状態となり、周辺機器インタフェース２１はディスクリプタを返せない状態になる。



【特許請求の範囲】
【請求項１】　ＵＳＢホストコントローラとＩＤを保持する記憶手段と認証手段とを有するコンピュータと、周辺機器の機能を実現する周辺機器機能実現手段とセキュリティ機能を実現するセキュリティ機能実現手段と前記周辺機器機能実現手段と前記セキュリティ機能実現手段とを切り替える機能制御手段とＩＤを保持する記憶手段とを有するＵＳＢ機器が接続され、前記ＵＳＢホストコントローラと前記周辺機器機能実現手段または前記セキュリティ機能実現手段との間で情報の授受を行なうセキュリティ機能付きＵＳＢ機器を備えたコンピュータシステムにおいて、
前記セキュリティ機能実現手段は、前記ＵＳＢ機器に保持されたＩＤを前記コンピュータに送信し、該認証手段は受信したＩＤと前記コンピュータに保持されたＩＤとを比較し、前記ＵＳＢ機器の前記コンピュータでの使用が認証された場合に、前記コンピュータから前記機能制御手段へ前記周辺機器機能実現手段に切り替えるためのコマンドを送信することを特徴とするセキュリティ機能付きＵＳＢ機器を備えたコンピュータシステム。
【請求項２】　請求項１に記載のセキュリティ機能付きＵＳＢ機器を備えたコンピュータシステムにおいて、前記機能制御手段は、前記コンピュータの電力状態が遷移するとき、前記セキュリティ機能実現手段に切り替えることを特徴とするセキュリティ機能付きＵＳＢ機器を備えたコンピュータシステム。
【請求項３】　請求項１に記載のセキュリティ機能付きＵＳＢ機器を備えたコンピュータシステムにおいて、前記コンピュータは、前記認証手段を有効または無効に設定する手段を有することを特徴とするセキュリティ機能付きＵＳＢ機器を備えたコンピュータシステム。
【請求項４】　請求項１に記載のセキュリティ機能付きＵＳＢ機器を備えたコンピュータシステムにおいて、前記ＵＳＢ機器は、前記セキュリティ機能実現手段を有効または無効に切り替える手段を有することを特徴とするセキュリティ機能付きＵＳＢ機器を備えたコンピュータシステム。
【請求項５】　請求項４に記載のセキュリティ機能付きＵＳＢ機器を備えたコンピュータシステムにおいて、前記セキュリティ機能実現手段を有効または無効に切り替える手段は、前記コンピュータでの有効または無効に切り替える操作または前記ＵＳＢ機器に設けられた有効または無効に切り替えるスイッチの操作に応じて、前記コンピュータから送信された前記セキュリティ機能実現手段を有効または無効に切り替えるコマンドにより有効または無効に切り替えられることを特徴とするセキュリティ機能付きＵＳＢ機器を備えたコンピュータシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、セキュリティ機能付きＵＳＢ機器を備えたコンピュータシステムに関し、より詳細には、コンピュータにＵＳＢ機器を接続して使用する際に、お互いに指定されたコンピュータやＵＳＢ機器のみ使用可能なセキュリティ機能付きＵＳＢ機器を備えたコンピュータシステムに関する。
【０００２】
【従来の技術】ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）は、パーソナルコンピュータの周辺機器の接続規格として、広く普及するようになった。ＵＳＢの特徴としては以下の（１）～（４）が挙げられ、これらがＵＳＢ機器の普及に寄与している。
（１）様々な種類の機器（入力機器，オーディオ機器，デジタルカメラ，ビデオカメラ，ネットワーク機器，プリンタ，スキャナ，ストレージ機器など）に対応した規格であること。
（２）様々な種類の機器が共通のコネクタを用いてパーソナルコンピュータと接続できること。
（３）プラグアンドプレイに対応し、活線挿抜が自由であること。
（４）１つのホストコントローラに対して最大１２７台までＵＳＢ機器の接続が可能であること。
【０００３】このような特徴を有するＵＳＢ機器は便利であるが、逆に言えば悪意を持ったユーザが、ＵＳＢ機器を接続し不正な使用を行なうことも容易ということになる。例えば、ストレージ機器を接続してデータの不正な読み書きなどを行なうといった操作を行なうことも容易ということになる。こういった問題点を解決するためには、ＵＳＢ機器に対して何らかのセキュリティ機能が必要である。
【０００４】パーソナルコンピュータに接続する機器についてのセキュリティに関する従来技術では、例えば、特開平１１－１８４７５６号公報（携帯情報端末におけるセキュリティ制御方法ならびにシステム及び同方法がプログラムされ記録される記憶媒体）というものがある。これは、携帯情報端末内部の不揮発性媒体に記録されている識別番号と接続先のパーソナルコンピュータに記憶されている識別番号との照合をパーソナルコンピュータ側で行い、携帯情報端末側での操作は不要というものである。
【０００５】また、特開平７－１２９７３６号公報（ＩＣメモリカード）というものもある。これは、ＩＣメモリカードの中にパスワードを記録した不揮発性媒体と、ユーザがパーソナルコンピュータから入力したパスワードが正しいか否かを判定する回路を持たせるというものである。不正と判定した場合はビジー信号を制御してビジー状態を保持することにより、読み書きを一切できないようにすることを提案している。しかし、ＵＳＢ機器についてのセキュリティについての提案はなかった。
【０００６】
【発明が解決しようとする課題】本発明は、上述のごと

き実情に鑑みてなされたもので、セキュリティ機能を有するＵＳＢ機器と該ＵＳＢ機器に対応したセキュリティ機能を有するコンピュータからなるセキュリティ機能付きＵＳＢ機器を備えたコンピュータシステムを提供することを目的としてなされたものである。

【０００７】また、セキュリティ機能を実現する手段が有効に機能するために、この手段が必ず最初にパーソナルコンピュータ側のＵＳＢホストコントローラから認識されるようにし、周辺機器としての本来の機能（ストレージ機器であればストレージの機能）を実現する手段が先に認識されてドライバがロードされ、一時的であっても認証処理より前にＵＳＢ機器の使用ができてしまうことを防止することを目的とする。

【０００８】更には、セキュリティ機能に対応しているコンピュータに対して通常は接続を許可していないＵＳＢ機器の接続を認める設定をも可能とし、例えば、セキュリティ機能に対応していないＵＳＢ機器を一時的に使用可能とすることを目的とする。

【０００９】更には、セキュリティ機能に対応しているＵＳＢ機器を通常は接続を許可していないパーソナルコンピュータへの接続を認める設定をも可能とし、例えば、セキュリティ機能に対応していないパーソナルコンピュータにセキュリティ機能に対応しているＵＳＢ機器を一時的に使用可能とすることを目的とする。

【００１０】

【課題を解決するための手段】請求項１の発明は、ＵＳＢホストコントローラとＩＤを保持する記憶手段と認証手段とを有するコンピュータと、周辺機器の機能を実現する周辺機器機能実現手段とセキュリティ機能を実現するセキュリティ機能実現手段と前記周辺機器機能実現手段と前記セキュリティ機能実現手段とを切り替える機能制御手段とＩＤを保持する記憶手段とを有するＵＳＢ機器が接続され、前記ＵＳＢホストコントローラと前記周辺機器機能実現手段または前記セキュリティ機能実現手段との間で情報の授受を行なうセキュリティ機能付きＵＳＢ機器を備えたコンピュータシステムにおいて、前記セキュリティ機能実現手段は、前記ＵＳＢ機器に保持されたＩＤを前記コンピュータに送信し、該認証手段は受信したＩＤと前記コンピュータに保持されたＩＤとを比較し、前記ＵＳＢ機器の前記コンピュータでの使用が認証された場合に、前記コンピュータから前記機能制御手段へ前記周辺機器機能実現手段に切り替えるためのコマンドを送信することを特徴としたものである。

【００１１】請求項２の発明は、請求項１の発明において、前記機能制御手段は、前記コンピュータの電力状態が遷移するとき、前記セキュリティ機能実現手段に切り替えることを特徴としたものである。

【００１２】請求項３の発明は、請求項１の発明において、前記コンピュータは、前記認証手段を有効または無効に設定する手段を有することを特徴としたものである。

【００１３】請求項４の発明は、請求項１の発明において、前記ＵＳＢ機器は、前記セキュリティ機能実現手段を有効または無効に切り替える手段を有することを特徴としたものである。

【００１４】請求項５の発明は、請求項４の発明において、前記セキュリティ機能実現手段を有効または無効に切り替える手段は、前記コンピュータでの有効または無効に切り替える操作または前記ＵＳＢ機器に設けられた有効または無効に切り替えるスイッチの操作に応じて、前記コンピュータから送信された前記セキュリティ機能実現手段を有効または無効に切り替えるコマンドにより有効または無効に切り替えられることを特徴としたものである。

【００１５】

【発明の実施の形態】以下に、本発明で提案するセキュリティ機能付きＵＳＢ機器を備えたコンピュータシステムの実施例について説明する。なお、以下、本発明書で説明するセキュリティ機能を持つパーソナルコンピュータをセキュリティ対応ＰＣ、セキュリティ機能を持つＵＳＢ機器をセキュリティ対応ＵＳＢ機器と呼ぶことにする。

【００１６】図１は、本発明の実施例のセキュリティ機能付きＵＳＢ機器を備えたコンピュータシステムを示す全体構成図である。コンピュータの構成要素としてＵＳＢの規格では「ＵＳＢクライアントソフトウェア」，「ＵＳＢシステムソフトウェア」，「ＵＳＢホストコントローラ」という３層の論理レイヤが定義されており、パーソナルコンピュータ１０においてもそれに従って、クライアントソフトウェア１１，ＵＳＢシステムソフトウェア１２，ＵＳＢバスインタフェース１３内のＵＳＢホストコントローラ１４を有する。更に、ＵＳＢバスインタフェース１３内には、ＵＳＢ機器との通信を行なうＳＩＥ（Ｓｅｒｉａｌ　Ｉｎｔｅｒｆａｃｅ　Ｅｎｇｉｎｅ）１５を有し、クライアントソフトウェア１１には、ＩＤ記憶部１６が接続されている。ＩＤ記憶部１６とは認証用のＩＤを保持する部分であり、専用の不揮発性メディアを用意してＩＤを書き込んでおく方法、Ｓｙｓｔｅｍ　ＢＩＯＳのＲＯＭの一部の領域を確保して書き込んでおく方法、オペレーティングシステムやデータファイルが存在するハードディスクにＩＤを書き込んでおくといった実現方法が考えられる。また、パーソナルコンピュータ１０は、表示部１７を備えている。表示部１７とは、例えば、ＣＲＴモニタなどである。

【００１７】コンピュータに接続される周辺機器の構成要素としてＵＳＢの規格では「ファンクション」，「ＵＳＢ論理デバイス」，「ＵＳＢバスインタフェース」という３層の論理レイヤが定義されており、ＵＳＢ機器２０においてもそれに従って周辺機器インタフェース（周辺機器の本来の機能を実現する手段）２１，論理デバイ

ス22，ＳＩＥからなるＵＳＢバスインタフェース２３を有する。なお、ファンクションとは、インタフェースが複数集合したものであり、インタフェースとは、ＵＳＢの規格では論理的な機能ことであり、ここでも同様の意味を持つものとして用いる。例えば、ＵＳＢプリンタにおいて、単方向（印字出力の機能のみ）と双方向の２つのモード（印字出力機能と、紙切れやインク切れのチェックなどステータスの読み出し機能）を持つ場合を考えると、このプリンタは、単方向モード、双方向モードという２つのインタフェースがあるといえる。また、論理デバイスとはエンドポイントの集まりである。そして、エンドポイントとは一種のＦＩＦＯ（Ｆｉｒｓｔ ｉｎ Ｆｉｒｓｔ ｏｕｔ）型のバッファメモリである。例えば、ＵＳＢプリンタでは、単方向モードには印刷機能用にエンドポイントが１つ、双方向モード用には印刷機能用とステータス読み出し機能用にエンドポイントが１つずつあるということになる。

【００１８】更に、ＵＳＢ機器２０は、セキュリティインタフェース（セキュリティ機能を実現する手段）２４と周辺機器インタフェース２１を制御するインタフェース制御部（機能制御手段）２５を有する。インタフェース制御部２５は、スイッチ２６を操作して、周辺機器インタフェース２１とセキュリティインタフェース２４を切り替えて、一方をディスクリプタを返せる状態に設定し、他方をディスクリプタを返せない状態に設定できる。セキュリティインタフェース２４には、認証用のＩＤを保持する不揮発性メディアからなるＩＤ記憶部２７が設けられている。また、ＵＳＢ機器２０には、セキュリティ機能切替スイッチ２８とセキュリティ機能ステータス表示部２９が備えられている。このセキュリティ機能切り替えスイッチ２８とは、ＵＳＢ機器２０のセキュリティ機能を有効または無効に切り替えるためのものであり、現在セキュリティ機能が有効か無効かがセキュリティ機能ステータス表示部２９に表示される。

【００１９】なお、ディスクリプタとは、プラグアンドプレイの機能をサポートするために、ＵＳＢの規格で規定された、ＵＳＢホストコントローラにおいてＵＳＢ機器のインタフェースに応じた最適なドライバがロードされるためにＵＳＢ機器からコンピュータに返すＵＳＢ機器のインタフェースの基本情報のことである。

【００２０】以下、パーソナルコンピュータ１０側でのセキュリティ対応／未対応、ＵＳＢ機器２０側でのセキュリティ対応／未対応の、各々の場合の組み合わせについて組み合わせパターン１～パターン３の２において説明する。

【００２１】組み合わせパターン１：セキュリティ対応ＰＣ１０にセキュリティ対応ＵＳＢ機器２０を接続する場合について説明する（請求項１，２）。図2は、本発明におけるセキュリティ機能付きコンピュータの状態遷移を説明するための図である。ＵＳＢ機器２０をセキュリティ対応ＰＣ１０に接続することにより、以下の処理が行われる。ＵＳＢホストコントローラ１４がＵＳＢ機器２０を認識すると（Ｓ１）、デバイスパワーステータスを設定する。ＵＳＢ機器２０がバスパワータイプのＵＳＢ機器である場合は、このときにＵＳＢ機器２０に電源が入る（Ｓ２）。次いで、セキュリティインタフェース２４のみがディスクリプタを返せるように初期設定する（Ｓ３）。外部電源を使うＵＳＢ機器であれば電源投入時の初期設定がこの状態となるようにしてもよい。

【００２２】パーソナルコンピュータ１０からＵＳＢ機器２０へインタフェース制御部２５の有無を確認するコマンドを送出して（Ｓ４）、ＵＳＢ機器２０はインタフェース制御部の有無を示す値を返し（Ｓ５）、パーソナルコンピュータ１０は戻り値を取得し、インタフェース制御部の有無を判定する（Ｓ６）。インタフェース制御部がある場合（Ｓ６－Ｙｅｓ）、パーソナルコンピュータから、セキュリティインタフェース２４のディスクリプタを要求する（Ｓ７）。仮に、パーソナルコンピュータにセキュリティ未対応のＵＳＢ機器を接続した場合は、インタフェース制御部がないと判定されるので（Ｓ６－Ｎｏ）、使用できないことをユーザに通知して終了する（Ｓ２１）。これにより接続が認められていないＵＳＢ機器の接続を防止することができる。

【００２３】ＵＳＢ機器２０はセキュリティインタフェース２４のディスクリプタを返す（Ｓ８）。セキュリティインタフェース２４のディスクリプタを取得できた場合（Ｓ９－Ｙｅｓ）、パーソナルコンピュータ１０からＵＳＢ機器２０へ認証用のＩＤを要求する（Ｓ１０）。ＵＳＢ機器２０はＩＤ記憶部２７内に保持しているＩＤを返す（Ｓ１１）。パーソナルコンピュータ１０はＩＤを取得し（Ｓ１２）、セキュリティインタフェース用のドライバをロードして（Ｓ１３）、パーソナルコンピュータ内のＩＤ記憶部１６に保持しているＩＤと照合して（例えば、両方のＩＤが一致するか判定して）、認証処理を行なう（Ｓ１４）。何らかの理由でＵＳＢ機器２０がセキュリティインタフェース２４のディスクリプタを返せなかった場合は（Ｓ９－Ｎｏ）、使用できないことをユーザに通知して終了する（Ｓ２１）。

【００２４】認証処理の結果、使用を認めると判断した場合は（Ｓ１５－Ｙｅｓ）、パーソナルコンピュータ１０からインタフェース制御部２５にコマンドを送出して（Ｓ１６）、周辺機器としての本来の機能（例えば、ＵＳＢ接続のストレージ機器でいえばストレージ機能）を実現する周辺機器インタフェース２１のディスクリプタを返せるようにする（Ｓ１７）。すなわち、周辺機器インタフェース２１側のスイッチ２６を閉じるということになる。パーソナルコンピュータ１０から、周辺機器インタフェース２１のディスクリプタを要求する（Ｓ１８）。ＵＳＢ機器２０は、周辺機器インタフェース２１のディスクリプタを返す（Ｓ１９）。パーソナルコンピ

ュータ１０は周辺機器インタフェース２１に応じた適切なドライバを選択しロードする（Ｓ２０）。これにより周辺機器インタフェース２１の使用が可能になる。なお、認証処理の結果、使用を認めないと判断した場合は（Ｓ１５－Ｎｏ）、使用できないことをユーザに通知して終了する（Ｓ２１）。

【００２５】図２には記載していないが、ＵＳＢ機器２０を取外す時と、ＵＳＢ機器２０を接続したままの状態であってもパーソナルコンピュータ１０のシステムのパワーステート（電力状態）を遷移させる時（シャットダウン，スタンバイ，休止状態）について説明する（請求項２）。この時は、パーソナルコンピュータ１０からインタフェース制御部２５にコマンドを送出して、周辺機器インタフェース２１のディスクリプタは返せないようにし、セキュリティインタフェース２４のディスクリプタを返せるような状態にする。これにより、取外したＵＳＢ機器２０を他のＰＣ（特に、セキュリティ機能に未対応のＰＣ）に接続すると認証処理なしに使用できてしまうという危険性をなくすことができる。ＵＳＢ機器２０を再度接続するときと、パーソナルコンピュータ１０のパワーステートを復帰させる場合は上述した図２の処理を行なうことになる。

【００２６】以上に説明したように、本発明では、ＵＳＢ機器にセキュリティ機能を実現する手段と、セキュリティ機能を実現する手段と周辺機器の機能を実現する手段とを切り替える手段と、ＩＤを保持する記憶手段を追加し、パーソナルコンピュータに認証手段と、ＩＤを保持する記憶手段を備えることで、ＵＳＢ機器を備えたコンピュータシステムにセキュリティ機能を付加し、悪意を持ったユーザの不正使用を防止できる。また、本発明では、接続が認められるまでは、周辺機器としての本来の機能（ＵＳＢプリンタであればプリンタの機能）のディスクリプタを返せないようにする確実なセキュリティ機能を付加できる。

【００２７】組み合わせパターン２：セキュリティ対応ＰＣにセキュリティ未対応ＵＳＢ機器を接続する場合について説明する（請求項３）。図３は、本発明におけるＰＣ側のセキュリティ機能の状態遷移を説明するための図である。セキュリティ対応ＰＣ１０にセキュリティ未対応ＵＳＢ機器を接続する場合は、下方向の矢印で示すように、ＰＣ１０側のセキュリティ機能を無効にする。ユーザはＰＣ１０上でクライアントソフトウェア１１の操作で認証処理を無効にする。これにより、セキュリティ未対応のＵＳＢ機器を問題なく使えるようになる。セキュリティ機能を再度有効にするためには、ＰＣ１０上でのクライアントソフトウェア１１の操作で認証処理を有効にし、上方向の矢印で示すように、セキュリティ機能を有効にする。

【００２８】以上に説明したように、セキュリティ機能を持たないＵＳＢ機器を組み合わせパターン１で述べたセキュリティ機能を有するパーソナルコンピュータに接続したことを検出した場合も、そのまま使用できる。

【００２９】組み合わせパターン３の１：セキュリティ未対応ＰＣにセキュリティ対応ＵＳＢ機器２０を接続する場合について説明する（請求項４および請求項５）。図４は、本発明におけるＵＳＢ機器側のセキュリティ機能の状態遷移を説明するための図である。セキュリティ未対応ＰＣにセキュリティ対応ＵＳＢ機器２０を接続する場合は、図４の（パターン３の１）と記載された部分の下方向の矢印で示すように、まず、セキュリティ対応ＰＣ１０に接続してセキュリティ対応ＵＳＢ機器２０のセキュリティ機能を無効した後にセキュリティ対応ＵＳＢ機器２０を取り外し、セキュリティ未対応のＰＣに接続する。

【００３０】セキュリティ対応ＵＳＢ機器２０に対するセキュリティ機能の無効化では、以下の順に処理を行なう。まず、セキュリティ対応ＵＳＢ機器２０をセキュリティ対応ＰＣ１０に接続する。セキュリティ対応ＰＣ１０はインタフェース制御部２５を認識して、セキュリティ機能に対応していることを認識する。セキュリティ対応ＰＣ１０からセキュリティ機能を有効または無効に切り替えるアプリケーションを起動してインタフェース制御部２５へコマンドを送出し、セキュリティインタフェース２４を無効にし、下方向の矢印で示すように、セキュリティ機能を無効にする。

【００３１】セキュリティ対応ＵＳＢ機器２０に対してセキュリティ機能を再度有効にする時は、以下の順に処理を行なう。まず、セキュリティ対応ＵＳＢ機器２０をセキュリティ対応ＰＣ１０に接続する。セキュリティ対応ＰＣ１０はインタフェース制御部２５を認識して、セキュリティ機能に対応していることを認識する。セキュリティ対応ＰＣ１０からセキュリティ機能を有効または無効に切り替えるアプリケーションを起動してインタフェース制御部２５へコマンドを送出し、セキュリティインタフェース２４を有効にし、上方向の矢印で示すように、セキュリティ機能を有効にする。

【００３２】以上に説明したように組み合わせパターン１で述べたセキュリティ機能を持つＵＳＢ機器をセキュリティ機能を持たないパーソナルコンピュータに接続して使用することが可能になる。

【００３３】組み合わせパターン３の２：セキュリティ未対応ＰＣにセキュリティ対応ＵＳＢ機器２０を接続する場合について説明する（請求項４および請求項５）。図４の（パターン３の２）と記載された部分の下方向の矢印で示すように、まず、パターン３の１と同様に、セキュリティ対応ＰＣ１０に接続してセキュリティ対応ＵＳＢ機器２０のセキュリティ機能を無効した後にセキュリティ対応ＵＳＢ機器２０を取り外し、セキュリティ未対応のＰＣに接続する。

【００３４】セキュリティ対応ＵＳＢ機器２０に対する

セキュリティ機能の無効化では以下の順に処理を行なう。まず、セキュリティ対応ＵＳＢ機器２０をセキュリティ対応ＰＣ１０に接続する。セキュリティ対応ＰＣ１０はインタフェース制御部２５を認識して、セキュリティ機能に対応していることを認識する。セキュリティ対応ＰＣ１０からセキュリティ機能切替スイッチ２８を操作した結果に応じたコマンドを送信して、セキュリティ機能を無効にし、下方向の矢印で示すように、セキュリティ機能を無効にする。

【００３５】セキュリティ対応ＵＳＢ機器２０に対してセキュリティ機能を再度有効にする時は、以下の順に処理を行なう。まず、セキュリティ対応ＵＳＢ機器２０をセキュリティ対応ＰＣ１０に接続する。セキュリティ対応ＰＣ１０はインタフェース制御部２５を認識して、セキュリティ機能に対応していることを認識する。セキュリティ対応ＰＣ１０からセキュリティ機能切替スイッチ２８を操作した結果に応じたコマンドを送信して、セキュリティ機能を有効にし、上方向の矢印で示すように、セキュリティ機能を有効にする。

【００３６】以上に説明したように、組み合わせパターン１で述べたセキュリティ機能を持つＵＳＢ機器をセキュリティ機能を持たないパーソナルコンピュータに接続して使用することが、スイッチを操作するという簡便な操作を行なうことで可能になる。

【００３７】

【発明の効果】請求項１の発明の効果

特定のコンピュータに対して特定のＵＳＢ機器のみの接続を認め、それ以外のＵＳＢ機器の使用を無効にすることができる。これにより、例えば、悪意を持ったユーザが、コンピュータにＵＳＢ機器を接続し不正な使用を行なうことを防止することができる。また、複数のユーザが使用するコンピュータを管理する管理者が、接続可能なＵＳＢ機器を管理するという目的にも使用できる。

【００３８】請求項２の発明の効果

コンピュータの電力状態が遷移するとき、ＵＳＢ機器をセキュリティ機能が有効になった状態とするので、周辺機器としての本来の機能が有効になった状態のＵＳＢ機器を、本発明によるセキュリティ機能を持たないパーソナルコンピュータに接続して使用される危険性がなくなるので、ＵＳＢ機器の無断持ち出しや盗難を防止することができる。

【００３９】請求項３の発明の効果

本発明のセキュリティ機能を持つパーソナルコンピュータのＩＤ認識機能を有効または無効に切り替え可能としたので、本発明によるセキュリティ機能を持つパーソナルコンピュータを本発明によるセキュリティ機能を持たないＵＳＢ機器と接続して使用することを一時的に認める場合にも対応することができる。

【００４０】請求項４，５の発明の効果

本発明のセキュリティ機能を持つＵＳＢ機器のセキュリティ機能を有効または無効に切り替え可能としたので、本発明によるセキュリティ機能を持たないコンピュータと、本発明によるセキュリティ機能を持つＵＳＢ機器とを接続して使用することを一時的に認める場合にも対応することができる。特に、請求項５の発明では、コンピュータ側のアプリケーションでの操作によりセキュリティ機能を無効にするので、新たなアプリケーションを追加するという簡便な方法でセキュリティ機能を有効または無効にすることができ、また、ＵＳＢ機器に設けたセキュリティ機能の切り替えスイッチによりセキュリティ機能を無効にするので、コンピュータ側のクライアントアプリケーション上での操作を煩わしいと感じるユーザには、セキュリティ機能を有効または無効にする操作に対する煩わしさを感じさせることがない。

【図面の簡単な説明】

【図１】　本発明の実施例のセキュリティ機能付きＵＳＢ機器を備えたコンピュータシステムを示す全体構成図である。

【図２】　本発明におけるセキュリティ機能付きコンピュータの状態遷移を説明するための図である。

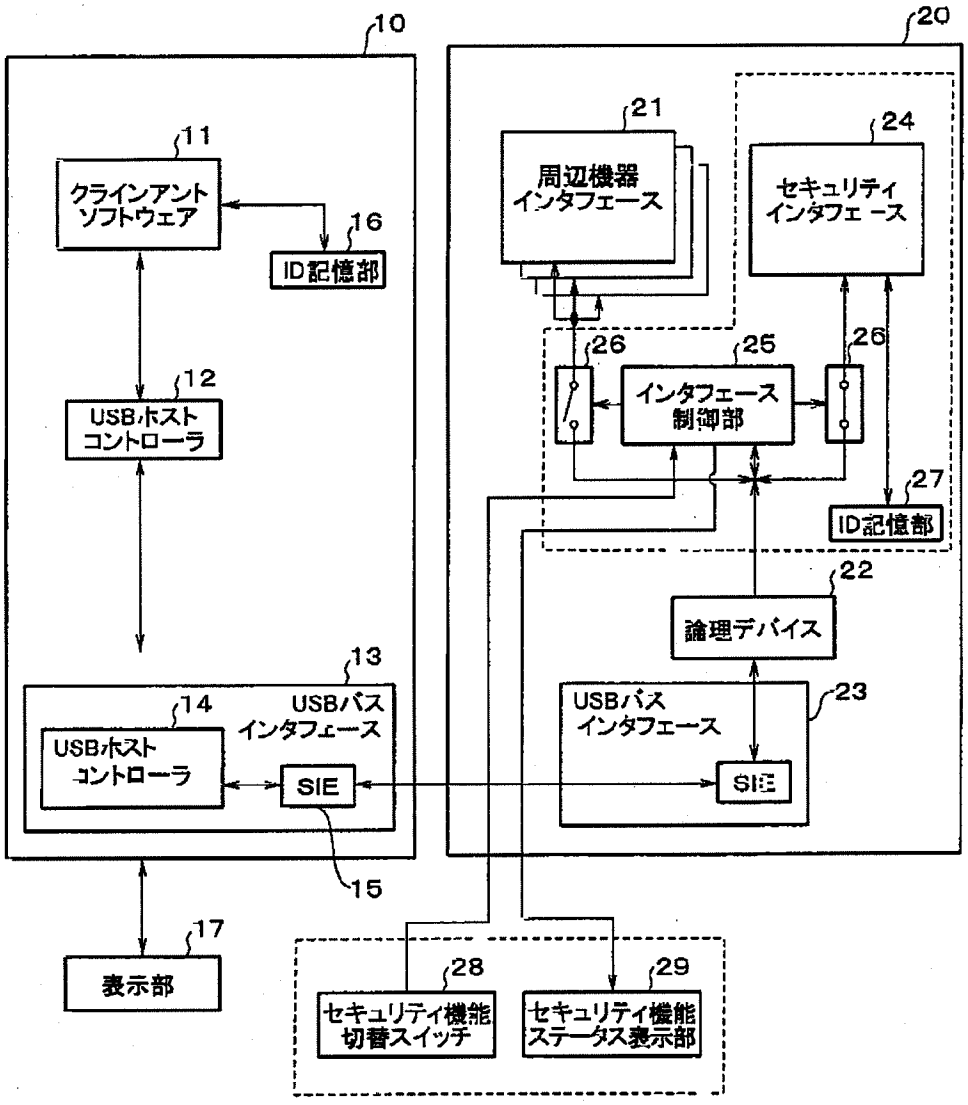
【図３】　本発明におけるＰＣ側のセキュリティ機能の状態遷移を説明するための図である。

【図４】　本発明におけるＵＳＢ機器側のセキュリティ機能の状態遷移を説明するための図である。

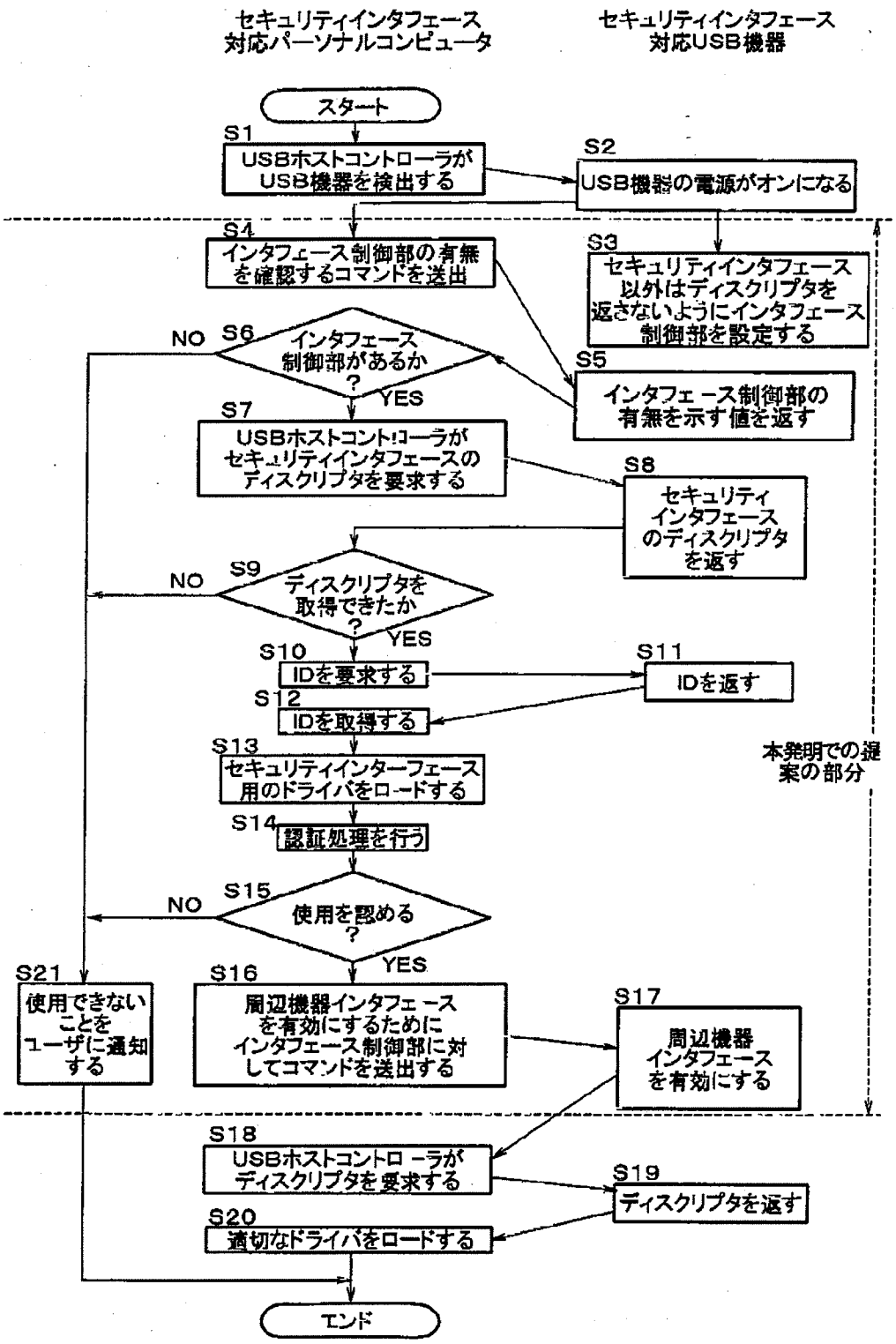
【符号の説明】

１０…パーソナルコンピュータ、１１…クライアントソフトウェア、１２…ＵＳＢシステムソフトウェア、１３…ＵＳＢバスインタフェース、１４…ＵＳＢホストコントローラ、１５…ＳＩＥ（Ｓｅｒｉａｌ　Ｉｎｔｅｒｆａｃｅ　Ｅｎｇｉｎｅ）、１６…ＩＤ記憶部、１７…表示部、２０…ＵＳＢ機器、２１…周辺機器インタフェース、２２…論理デバイス、２３…ＵＳＢバスインタフェース、２４…セキュリティインタフェース、２５…インタフェース制御部、２６…スイッチ、２７…ＩＤ記憶部、２８…セキュリティ機能切替スイッチ、２９…セキュリティ機能ステータス表示部。

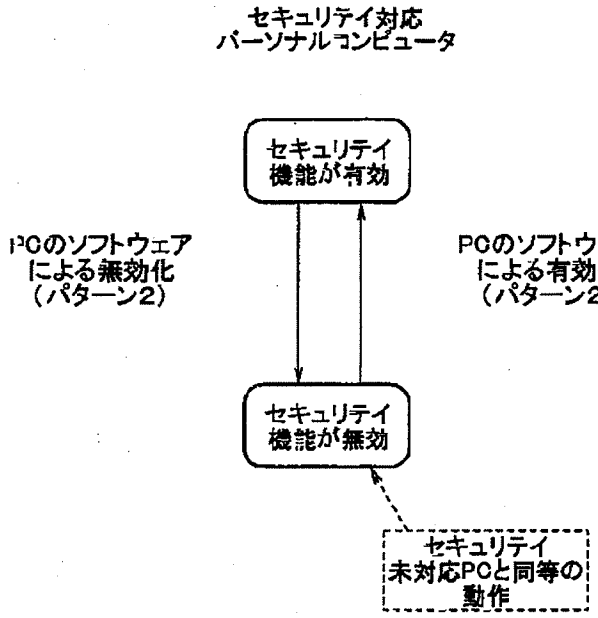
【図1】


10
20
11
クラインアント
ソフトウェア
16
ID記憶部
12
USBホスト
コントローラ
13
14
USBホスト
コントローラ
USBバス
インタフェース
SIE
15
17
表示部
21
周辺機器
インタフェース
24
セキュリティ
インタフェース
26
25
インタフェース
制御部
26
27
ID記憶部
22
論理デバイス
USBバス
インタフェース
23
SIE
28
セキュリティ機能
切替スイッチ
29
セキュリティ機能
ステータス表示部

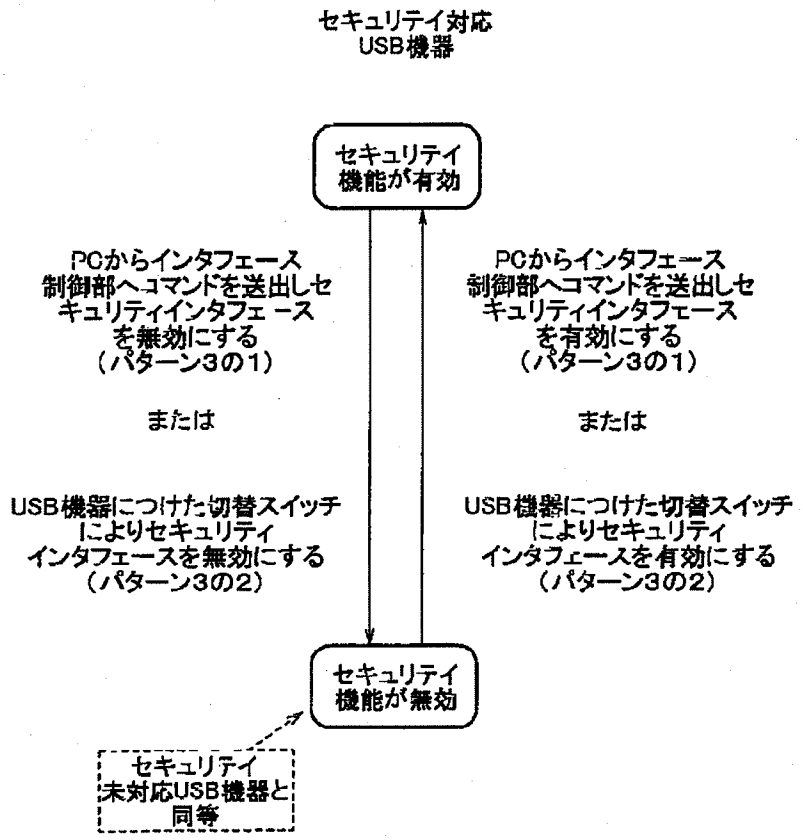
【図2】


セキュリティインタフェース
対応パーソナルコンピュータ
セキュリティインタフェース
対応USB機器
スタート
S1
USBホストコントローラが
USB機器を検出する
S2
USB機器の電源がオンになる
S4
インタフェース制御部の有無
を確認するコマンドを送出
S3
セキュリティインタフェース
以外はディスクリプタを
返さないようにインタフェース
制御部を設定する
NO
S6
インタフェース
制御部があるか
?
YES
S5
インタフェース制御部の
有無を示す値を返す
S7
USBホストコントローラが
セキュリティインタフェースの
ディスクリプタを要求する
S8
セキュリティ
インタフェース
のディスクリプタ
を返す
NO
S9
ディスクリプタを
取得できたか
?
YES
S10
IDを要求する
S11
IDを返す
S12
IDを取得する
S13
セキュリティインターフェース
用のドライバをロードする
S14
認証処理を行う
本発明での提
案の部分
NO
S15
使用を認める
?
YES
S21
使用できない
ことを
ユーザに通知
する
S16
周辺機器インタフェース
を有効にするために
インタフェース制御部に対
してコマンドを送出する
S17
周辺機器
インタフェース
を有効にする
S18
USBホストコントローラが
ディスクリプタを要求する
S19
ディスクリプタを返す
S20
適切なドライバをロードする
エンド

【図3】


セキュリティ対応
パーソナルコンピュータ
セキュリティ
機能が有効
PCのソフトウェア
による無効化
（パターン2）
PCのソフトウェア
による有効化
（パターン2）
セキュリティ
機能が無効
セキュリティ
未対応PCと同等の
動作

【図4】


セキュリティ対応
USB機器
セキュリティ
機能が有効
PCからインタフェース
制御部へコマンドを送出しセ
キュリティインタフェース
を無効にする
（パターン3の1）
または
USB機器につけた切替スイッチ
によりセキュリティ
インタフェースを無効にする
（パターン3の2）
PCからインタフェース
制御部へコマンドを送出しセ
キュリティインタフェース
を有効にする
（パターン3の1）
または
USB機器につけた切替スイッチ
によりセキュリティ
インタフェースを有効にする
（パターン3の2）
セキュリティ
機能が無効
セキュリティ
未対応USB機器と
同等